NPDB-HIPDB DATA BANK NEWS

U.S. Department of Health and Human Services
HRSA
Health Resources and Services Administration

National Practitioner Data Bank—Healthcare Integrity and Protection Data Bank

OCTOBER 2010

DPDB Helping States Maintain Reporting Compliance

Maintaining complete and accurate information in the Healthcare Integrity and Protection Data Bank (HIPDB) is a top priority for the Health Resources and Services Administration (HRSA). In March 2010 HRSA's Division of Practitioner Data Banks (DPDB) began implementing a multi-phase plan to monitor the reporting activities of all organizations required to report to the Data Banks. Compliance monitoring will be ongoing to assure that accurate and up-to-date information is available to all Data Bank users. Our initial results were posted on the Data Banks Web site on July 1, 2010, and will be updated periodically. To view the Reporting Compliance Status of Government Agencies, visit *www.npdb-hipdb.hrsa.gov.*

COMPLIANCE PLAN
The first phase of the plan focused on 13 State nursing boards which were the subject of an article in the *Los Angeles Times*. A comparison of data obtained from the State boards and the HIPDB resulted in a list of potentially missing reports. The State boards were sent a request to reconcile the data.

The next phase of the plan focused on States and Territories that appeared to have never reported on professions that are licensed, certified or authorized by that State

Upcoming Data Bank Improvements

IDENTITY-PROOFING
Planning is well underway for significant changes to user registration and renewal processes which will entail identity-proofing of all Data Bank users. The new identity-proofing process, called electronic authentication or e-authentication, is scheduled for a phased-in implementation beginning in January 2011. All certifying officials, Entity Data Bank Administrators, and users will have to provide proof of identity and organizational affiliation when registering or renewing their entities with the Data Banks. Entity Data Bank Administrators and certifying officials will also be required to have their identities verified by a Notary due to their higher level of responsibility.

What is e-authentication? Electronic authentication (e-authentication) is "the process of establishing

confidence in user identities electronically presented to an information system." The new guidelines establish more stringent security measures, assuring that any user who is given access to the Data Banks is who he says he is. Identity assurance has become essential as technology has evolved to the point where it is today–people all around the country are accessing remote computer systems over the Internet that are located at a distance from their users.

The e-authentication initiative is responsive to the Government Paperwork Elimination Act of 1998 (GPEA). The principles followed in implementing this enhancement are the security standards published by the National Institute of Standards and Technology (NIST) in Special Publication 800-63-1 ("Electronic Authentication Guideline"). In this document, NIST describes the technical

DPDB Helping States Maintain Reporting Compliance...continued from page 1

or Territory. HRSA requested that each of these State boards provide an explanation for the absence of reports and, as appropriate, provide a corrective action plan to submit the necessary information.

In addition to focusing on State boards that had never reported to the HIPDB, HRSA identified six professions that are most frequently queried by hospitals: nursing-related professions, physician assistants, podiatrists, pharmacists, social workers, and psychologists. For these professional areas, HRSA compared data obtained from the State boards with reports in the HIPDB. This resulted in a list of potentially missing reports. The State boards were sent a request to reconcile the data and, as appropriate, provide a corrective action plan to submit the missing information.

Along with implementing the compliance plan, DPDB conducted seven technical assistance conference calls with more than 400 participants from all 50 States to answer Data Bank reporting questions. For State boards wishing to perform their own audit, DPDB provided them with their HIPDB data. DPDB looks forward to working with each State board to assist them in meeting the reporting requirements.

RESULTS
Each phase of the compliance plan improved the completeness and accuracy of reports in the Data Banks. The number of reports also increased. Between February 1, 2010 and June 21, over 72,000 reports were submitted to the Data Banks. This 4-month total during 2010 represents nearly double the number of reports submitted over all 12 months in 2009.

NEXT STEPS
While these initial efforts have increased compliance with required reporting to the Data Banks, our monitoring activities have really only just begun. DPDB will continue to monitor reporting compliance of State agencies. Also, we will examine adverse action reports of nine professions beyond the first six included in our initial efforts. Additional future activities will involve auditing other mandatory reporters (e.g., medical malpractice payers) as well as mandatory queriers. The next compliance status posting on the Data Banks Web site will occur no later than October 1, 2010, with periodic updates expected thereafter.

HRSA'S COMMITMENT
HRSA is committed to improving the completeness and accuracy of information in the Data Banks. Newly enhanced compliance monitoring activities are part of our continuing mission to protect the health and safety of the public. ❖

Upcoming Data Bank Improvements...continued from page 1

requirements that must be met by Federal agencies that allow remote users to access their information systems. Based upon ongoing security evaluations of these systems and review of these requirements, National Practitioner Data Bank (NPDB) and the Healthcare Integrity and Protection Data Bank (HIPDB) are systems that require identity-proofing for all users.

How will e-authentication affect you? The identity-proofing process will apply to organizations registering with the Data Banks for the first time. In addition, an organization's first renewal after e-authentication takes effect will entail identity-proofing of the Entity Data Bank Administrator, the certifying official, and all users. The new authentication procedures will also require certifying officials, Entity Data Bank Administrators, and users to provide proof to the Data Banks that they are employed by the organization requesting renewal. The Entity Data Bank Administrator will become a Local Registration Authority (LRA) for onsite users. A LRA is tasked with reviewing and approving users' identification documents and sending those documents on to the Data Banks.

OTHER NEW FEATURES
January 2011 changes incorporate a number of new features that will benefit Entity Data Bank Administrators. Some enhancements are specifically related to the e-authentication effort; whereas others represent changes requested by users. Enhancements to watch for include:

- System-generated emails to users to notify them of their new accounts.

- A sortable, filterable listing on-screen of an organization's users, with new columns for status and role.

- New functionalities for Entity Data Bank Administrator accounts. Entity Data Bank Administrators will be able to create additional Entity Data Bank Administrator accounts as well as User accounts and use their accounts to perform regular Data Bank activities. A second account will no longer be needed.

- Ability to indicate roles for each user account, e.g. billing, querying.

Watch for further updates about these new initiatives as January 2011 approaches. ❖

Security Hints from the Data Banks

Test your security knowledge! Respond True or False (T or F) to the Data Bank questions below:

1. When you create a password, use personal information (your birth date, a pet's name, etc.) so that you will be able to remember your password easily. T or F

2. You should avoid downloading or installing personal software onto your work computer. T or F

3. Documents containing sensitive information or Personally Identifiable Information (PII) should be retrieved from office printers as soon as possible. T or F

4. An email from a known organization requesting personal information, such as your account number or password, is always legitimate. T or F

5. If your laptop is password-protected, it is safe to leave it unattended for a few minutes in a public place. T or F

ANSWERS:

1. **False**. Passwords containing your personal information will be extremely easy to guess, making it possible for someone to hack into your account. Instead, create a password that is easy for you to remember, but meaningless to someone else. To help you create strong passwords, the Data Banks enforce the following password rules:

   a. A changed or updated password must contain between 8 and 14 characters, with at least 1 alphabetic and 1 numeric character.
   b. Password must be different from previous 4 passwords.
   c. Password must not be similar to a word in the dictionary.
   d. Password must not be similar to a common Data Bank phrase.
   e. Password must not be similar to your user ID.
   f. Password must not be a simple sequence of characters (e.g., abcd1234).
   g. Changed or updated password expires after 90 calendar days.

2. **True**. Downloading programs to your computer (on purpose or inadvertently) can create problems for your computer and for the office network. Even a seemingly harmless screensaver or game can do damage: do not download it. In addition, a file-sharing program, like iTunes, is not permissible in most office environments; these types of programs are security breaches waiting to happen.

3. **True**. Never leave sensitive documents on the office printer or copy machine. Always pick up print jobs immediately so that unauthorized people cannot view your sensitive information.

4. **False**. A legitimate business will never ask for personal information via email. This type of request is most likely a "spear phishing" attack targeting an individual, where the attack appears to be from a trusted source. The Data Banks will never request confidential or personal information from you via email.

5. **False**. Never take a chance on leaving your work laptop unattended. To leave it in a public place invites theft and to leave it unsecured anyplace invites hackers. A hacker can crack your password and obtain access to all the files on your computer. Your laptop should always be stored securely out of sight, preferably in a form-fitting sleeve to protect the laptop, and then placed in a briefcase, backpack, or tote.❖

Let PDS Help with Credentialing

The Proactive Disclosure Service (PDS) is a notification service that assists medical staffing professionals with credentialing their practitioners. Unlike traditional Data Bank querying, which requires you to submit a query every time you want to conduct a review, PDS does the work for you. It is continually on duty, monitoring the Data Banks for new or revised reports on your practitioners, and letting you know promptly if there is anything new you should know about.

The credentialing process can be time-consuming, especially if you have many practitioners and are required by law to query the Data Banks. Things can change during the period of time between credentialing cycles, and PDS informs you as those changes occur. Enrolling your practitioners in PDS also fulfills certain accreditation standards. The Joint Commission, the Utilization Review Accreditation Commission (URAC), the Commission on Accreditation of Rehabilitation Facilities (CARF), and the National Committee for Quality Assurance (NCQA) have all endorsed PDS.

Effortless querying and more. PDS automatically monitors your practitioners, and also offers:

- Prompt notice of new reports on your practitioners in addition to changes to past reports. If new reports are submitted for an enrolled practitioner, PDS will let you know about them within 24 hours, without any querying on your part. Both PDS and traditional queries provide you with a "snapshot" of adverse actions at the initial time of querying, but only PDS keeps that snapshot up-to-date by letting you know about new reports that may occur later.

- Printable enrollment confirmations for newly-enrolled and renewed PDS subjects. PDS enrollment confirmations demonstrate compliance with continuous monitoring standards.

- Advance scheduling of practitioner cancellation from PDS. If you know the date a practitioner or group of practitioners will be leaving your facility, you can enter their name(s) and departure date(s) in advance. PDS will automatically cancel the enrollments when the time comes.

- An *Enrollment Confirmation* screen that offers enhanced sorting and filtering capabilities. Sort or filter your enrolled practitioners by renewal date, department, or status. Clicking a practitioner name in the list will take you to the *Subject Detail* screen, making it a cinch to keep physician profiles up-to-date.

- Ability to print ad hoc enrollment confirmations anytime for individual or selected groups of enrolled practitioners. These on-demand confirmations give you an up-to-the-minute collection of all reports on file for the selected enrollees.

- Value-added benefits. At $3.25 per year, per practitioner per Data Bank, PDS is well worth the benefit of knowing you are always up-to-date.

Ready to come on board? Join the 1,500+ organizations already using PDS. PDS is available to all users who are eligible to query the Data Banks. Activating PDS is a simple three-step process that any Entity Data Bank Administrator can do in minutes:

1. Sign in to the Data Banks and click **Activate PDS** on the *Administrator Options* screen.

2. Complete the *Activate Proactive Disclosure Service* form and indicate which users should receive the monthly summary emails.

3. Click **Submit to Data Bank(s)** and begin enrolling practitioners in PDS.

If your facility uses an agent, you will be happy to know that agent relationships are unaffected by PDS activation and require nothing special during the PDS setup. You will find instructions along with other information about PDS, including fee specifics and screen shots, at our Web site: *www.npdb-hipdb.hrsa.gov/pds.html*. As always, the Customer Service Center welcomes the opportunity to assist you. Call 1-800-767-6732 between the hours of 8:30 a.m. and 6:00 p.m. (5:30 on Fridays), any weekday except Federal holidays, to speak with an Information Specialist. ❖

We frequently update our schedule so please also refer to our Web site, *www.npdb-hipdb.hrsa.gov/outreach.html.*❖

RECENT OUTREACH ACTIVITIES

CONFERENCE	LOCATION	DATE
Missouri Association of Medical Staff Services (MOAMSS) Summer Conference	Kansas City, MO	July 15-16, 2010
National Conference of State Legislators (NCSL) Annual Legislative Summit	Louisville, KY	July 25-28, 2010
New Mexico Association of Medical Staff Services (NMAMSS) Fall Conference	Albuquerque, NM	August 20, 2010
Mississippi Association of Medical Staff Services (MSAMSS)	Madison, MS	August 26, 2010
Data Bank Education Forum	Chicago, IL	Sept. 16, 2010
Administrators in Medicine (AIM) Eastern & Southern Regional Meeting	Baltimore, MD	Sept. 23, 2010
Council of Licensure Enforcement & Regulation (CLEAR) Annual Conference	Nashville, TN	Sept. 23-25, 2010

UPCOMING OUTREACH ACTIVITIES

CONFERENCE	LOCATION	DATE	ROLE
National Association of Medical Staff Services (NAMSS) 34th Annual Conference and Exhibition	Orlando, FL	October 2-6, 2010	Speaker/Exhibitor
Federation of Associations of Regulatory Boards (FARB) 18th Annual Attorney Certification Seminar in Professional Regulatory Law	Washington, DC	October 3, 2010	Speaker
American Association of Dental Boards (AADB) Annual Meeting Attorney Roundtable	Orlando, FL	October 7, 2010	Speaker
National Board for Certification in Occupational Therapy Annual State Regulatory Conference	Indianapolis, IN	October 23, 2010	Speaker
Ohio Association of Medical Staff Services (OAMSS) Fall Conference	Columbus, OH	October 29, 2010	Speaker
Physicians Insurers Association of America (PIAA) Corporate Counsel Section Workshop	San Diego, CA	November 5, 2010	Speaker
Alabama Association of Medical Staff Services (AAMSS)	Birmingham, AL	November 5, 2010	Speaker
National Committee for Quality Assurance (NCQA) Annual Meeting	Washington, DC	December 4, 2010	Speaker
Indiana Association of Medical Staff Services Quarterly Educational Conference	Lafayette, IN	January 28, 2011	Speaker

Spotlight on Factually Sufficient Narrative Descriptions...Did You Know?

Did you know...that Data Bank reports must include a factually sufficient narrative description?

If you are a Data Bank reporter, then you should know the importance of a factually sufficient narrative description. Statutory reporting requirements dictate that all Adverse Action Reports contain a factually sufficient narrative description. While the description does not have to be lengthy, the narrative must clearly describe the act(s), omission(s), reasons, and circumstances of the action being reported. In addition, it should be easily understood by a knowledgeable observer.

When crafting a factually sufficient narrative, it is not enough to simply repeat the language of the Basis for Action codes. Instead you need to include details of the event leading up to the adverse action and provide an explanation about what the practitioner did to warrant the report. The narrative is helpful to subsequent queriers who read the report. If the report includes multiple Adverse Action Codes, the reporter should describe the relationships between the multiple codes. Committee or Board official findings or orders are generally the best source for language when composing narratives.

NARRATIVE DESCRIPTION TIPS:

- May contain up to 4,000 characters including spaces and punctuation;

- May only reference others by title or relationship (the Chief of Staff, the patient's spouse);

- May **not** include personally identifying information (PII) about patients, other healthcare practitioners, plaintiffs, and/or witnesses (e.g., names);

- May **not** include links to other Web sites; and

- Should avoid using inflammatory or emotive language.

If the narrative is longer than 4,000 characters it will be truncated. If the narrative includes PII, then that information will be redacted. Below are three examples of a factually sufficient narrative:

1. Type of Action: **Voluntary Surrender of License**
   Action: Voluntary Surrender of License (1145)
   Basis for Action: Unable to Practice Safely by Reason of Alcohol or Other Substance Abuse (F2), Diversion of Controlled Substances (H6)
   Narrative: The Board was investigating this practitioner for allegedly diverting drugs for personal use. To avoid further investigation, she voluntarily surrendered her license. The practitioner also agreed to the surrender of her right to reapply for a license for a minimum of two (2) years.

2. Type of Action: **Licensure Action**
   Action: Publicly Available Negative Action or Finding, specify Letter of Warning (1189)
   Basis for Action: Failure to Comply With Continuing Education or Competency Requirements (A2), Unprofessional Conduct (10)
   Narrative: Violation of State Code Section 432(b): failure to meet continuing education requirements. By State Code, failure to meet continuing education requirements is considered to be "unprofessional conduct."

3. Type of Action: **Clinical Privilege Action**
   Action: Suspension of Privileges (1630)
   Basis for Action: Immediate Threat to Health or Safety (F1)
   Narrative: Privileges were suspended for six (6) months and the physician was placed on probation for two (2) years for failing to maintain sterile conditions in the operating room and by neglecting to wash hands between patients.

For other tips and examples, see our *Fact Sheet on Submitting a Factually Sufficient Narrative Description*, located at *www.npdb-hipdb.hrsa.gov/pubs/fs/Fact_Sheet-Submitting_a_Factually_Sufficient_Narrative_Description.pdf*. ❖

Dear Data Banks...

This column answers questions about Data Bank policies and procedures. If you have a question, please email your question to "Dear Data Banks" at *help@npdb-hipdb.hrsa.gov.* We look forward to hearing from you!

Question: I am preparing to enroll practitioners in the Proactive Disclosure Service (PDS). Do I have to enroll all of my practitioners at the same time, or can I enroll some of my practitioners today and others in a few months?

Answer: You may enroll your practitioners at different times if you wish. The enrollment period is 12 months and there are no restrictions on the number of practitioners that you may enroll or when you enroll them. The PDS will keep track of renewal dates for you for all your practitioners regardless of when they are enrolled.

Question: Now that the National Practitioner Data Bank (NPDB), Section 1921 is open for querying and reporting, can you provide examples of "other health care practitioners" and "health care entities" that State licensing authorities must report to the NPDB?

Answer: "Other health care practitioners" might include chiropractors, nurses, social workers, and podiatrists, for example. "Other health care entities" could include long-term care facilities and ambulatory surgery centers.

Question: My organization, which requires its physicians to be board certified, denied a physician's application for surgical privileges because the physician was not board certified. Is this action reportable to the NPDB?

Answer: No, in this case, the action is not reportable. If the health care organization's policy requires board certification, the automatic or administrative denial of medical staff membership or of a clinical privilege is not reportable.

Adverse actions related to medical staff membership or clinical privileges that are reportable to the NPDB, are those resulting from professional review of a practitioner's competence or professional conduct.

Question: Can you tell me the types of actions that private accreditation organizations are required to report under Section 1921 of the Social Security Act?

Answer: Private accreditation entities are required to report final denials or terminations of accreditation that result from risks to patient safety or concerns about quality of health care services.

Question: Can you clarify what types of NPDB users, under Section 1921 of the Social Security Act, have access to State licensure actions on all health care practitioners and health care entities?

Answer: Private-sector hospitals and health care entities now have access to the additional licensure information contained under Section 1921 of the NPDB. Additionally, State health care licensing boards for practitioners and entities, agencies administering Federal health care programs or their contractors, State agencies administering State health care programs, Quality Improvement Organizations, State Medicaid Fraud Control Units, U.S. Comptroller General, U.S. Attorney General, and other law enforcement agencies may query under Section 1921 of the NPDB.

Question: If a physician does not know that she is under investigation for possible professional incompetence and resigns from a hospital, is her resignation reportable to the NPDB?

Answer: Yes. Regardless of whether the practitioner is aware that an investigation is being conducted, her resignation or surrender of privileges must be reported if she was under investigation at the time of the resignation or surrender. The reporting organization must be able to produce evidence that an investigation was ongoing at the time of the resignation or surrender, in order to support the report. Resignations and surrenders must also be reported in situations where a practitioner resigns or surrenders privileges after being notified that an investigation will be conducted, but before the investigation actually begins.

If you would prefer to discuss a specific issue, please call the Customer Service Center at 1-800-767-6732. Information Specialists are available to speak with you weekdays from 8:30 a.m. to 6:00 p.m. (5:30 p.m. on Fridays) Eastern Time. The Customer Service Center is closed on all Federal holidays.❖

Topic of the Quarter

Do you have a process in place for when you receive your PDS notifications? If so, we would like to hear your story! Help other PDS users by sharing your tips and the processes that work for your organization. Please send the Data Banks your story via email, at *help@npdb-hipdb.hrsa.gov*, with the subject "PDS Story," and we will contact you about possibly publishing it in an upcoming issue of Data Bank News. ❖

On the Horizon

A New Look

Watch for the newly redesigned NPDB-HIPDB Web site. The new site is even more user friendly and designed so that whether you are a health care organization, practitioner, or just interested in Data Bank News, you can easily find the information you need. The Web redesign is the culmination of over a year-long effort. We look forward to your feedback on the new look.

Electronic Delivery of the Data Bank Newsletter

Help the Data Banks in their continuing effort to "go green" by only receiving the Data Bank News electronically. You already receive an email notifying you of each issue. You can view each issue and download it to your computer, or print it if you wish. Each newsletter (including archived issues) is currently available on our Web site at *www.npdb-hipdb.hrsa.gov/newsletter.html* and can be easily shared among peers. ❖

U.S. DEPARTMENT OF HEALTH AND
HUMAN SERVICES

Health Resources and Services Administration
Bureau of Health Professions
Division of Practitioner Data Banks
Parklawn Building, Room 8-103
5600 Fishers Lane
Rockville, MD 20857